

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Ryo OCHI, et al.

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: ENCRYPTION PROCESSING APPARATUS, ENCRYPTION PROCESSING METHOD, AND COMPUTER PROGRAM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- Full benefit of the filing date of U.S. Application Serial Number _____, filed _____, is claimed pursuant to the provisions of 35 U.S.C. §120.
- Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. _____ Date Filed _____
- Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

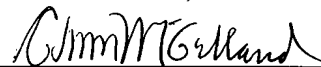
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-001647	January 8, 2003

Certified copies of the corresponding Convention Application(s)

- are submitted herewith
- will be submitted prior to payment of the Final Fee
- were filed in prior application Serial No. _____ filed _____
- were submitted to the International Bureau in PCT Application Number _____
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- (A) Application Serial No.(s) were filed in prior application Serial No. _____ filed _____ ; and
- (B) Application Serial No.(s) _____
 - are submitted herewith
 - will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle

Registration No. 40,073

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 月 8 日
Date of Application:

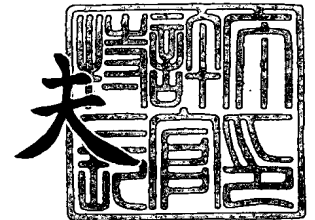
出 願 番 号 特 願 2 0 0 3 - 0 0 1 6 4 7
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 0 1 6 4 7]

出 願 人 ソニー株式会社
Applicant(s):

2 0 0 3 年 1 1 月 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0290676406

【提出日】 平成15年 1月 8日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
 内

 【氏名】 越智 龍

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
 内

 【氏名】 日下部 進

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100093241

 【弁理士】

 【氏名又は名称】 宮田 正昭

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100101801

 【弁理士】

 【氏名又は名称】 山田 英治

 【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号処理装置、および暗号処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項 1】

データ暗号処理を実行する暗号処理装置であり、
オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割し、各設定群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する制御部と、
前記制御部の設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理部と、
を有することを特徴とする暗号処理装置。

【請求項 2】

前記制御部は、
前記分割群の少なくともいずれかの群に、前記オリジナル暗号処理シーケンスには不要なダミーの暗号処理を実行するダミー暗号処理単位を設定し、該ダミー暗号処理単位を含む複数群の暗号処理単位の攪拌を実行して1つの攪拌暗号処理シーケンスを設定する構成であることを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 3】

前記制御部は、
1以上の暗号処理単位から構成される複数の群への分割処理において、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、該独立実行可能なシーケンスを単位とした分割群の設定処理を実行する構成であることを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 4】

前記暗号処理単位は、シングルDES暗号処理であり、
前記制御部は、1以上のシングルDES暗号処理を含むオリジナル暗号処理シ

ーケンスを 1 以上のシングルDES暗号処理から構成される複数の群に分割して、各分割群に含まれるシングルDES暗号処理単位を各設定群内での処理順を固定とする条件の下で、各設定群のシングルDES暗号処理単位の相互入れ替えにより攪拌し、1つの攪拌暗号処理シーケンスを設定する構成であることを特徴とする請求項1に記載の暗号処理装置。

【請求項5】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、

前記制御部は、

トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行する構成であることを特徴とする請求項1に記載の暗号処理装置。

【請求項6】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理および乱数生成処理を含む暗号処理シーケンスであり、

前記制御部は、

乱数生成処理を3回のシングルDES処理による変換処理を含む処理として構成し、分割群のいずれかに乱数生成処理としてのトリプルDES暗号処理を設定する構成としたことを特徴とする請求項1に記載の暗号処理装置。

【請求項7】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、

前記制御部は、

トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行するとともに、前記分割群の少なくともいずれかの群に、本来のオリジナル暗号処理シーケンスには不要なダミー暗号処理としてのダミーのシングルDES処理を設定し、設定するダミーのシングルDES処理数をトリプルDESに対応する3の倍数として設定する構成としたことを特徴とする請求項1に記載の暗号処理装置

。

【請求項 8】

前記暗号処理装置は、

前記制御部の設定した攪拌暗号処理シーケンスを構成する暗号処理単位の処理結果を格納するメモリを有し、

前記制御部は、前記メモリに対して、いずれの暗号処理単位の処理結果であるかを識別可能な態様で処理結果の格納を実行する構成であることを特徴とする請求項 1 に記載の暗号処理装置。

【請求項 9】

データ暗号処理を実行する暗号処理装置であり、

オリジナル暗号処理シーケンスを、1 以上の暗号処理単位に分割し、前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する制御部と、

前記制御部の設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理部と、

を有することを特徴とする暗号処理装置。

【請求項 10】

前記オリジナル暗号処理シーケンスに含まれる暗号処理単位は、シングルDES暗号処理であり、

前記制御部は、

前記ダミー暗号処理単位をシングルDES暗号処理として設定する構成であることを特徴とする請求項 9 に記載の暗号処理装置。

【請求項 11】

データ暗号処理を実行する暗号処理方法であり、

オリジナル暗号処理シーケンスを、1 以上の暗号処理単位から構成される複数の群に分割する分割ステップと、

前記分割ステップにおいて設定した各群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを

設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンス設定ステップにおいて設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、
を有することを特徴とする暗号処理方法。

【請求項 12】

前記暗号処理方法は、さらに、

前記分割群の少なくともいずれかの群に、前記オリジナル暗号処理シーケンスには不要なダミーの暗号処理を実行するダミー暗号処理単位を設定するステップを含み、

前記攪拌暗号処理シーケンス設定ステップは、

前記ダミー暗号処理単位を含む複数群の暗号処理単位の攪拌を実行して1つの攪拌暗号処理シーケンスを設定することを特徴とする請求項 11 に記載の暗号処理方法。

【請求項 13】

前記分割ステップは、

1以上の暗号処理単位から構成される複数の群への分割処理において、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、該独立実行可能なシーケンスを単位とした分割群の設定処理を実行するステップであることを特徴とする請求項 11 に記載の暗号処理方法。

【請求項 14】

前記暗号処理単位は、シングルDES暗号処理であり、

前記分割ステップは、

1以上のシングルDES暗号処理を含むオリジナル暗号処理シーケンスを1以上のシングルDES暗号処理から構成される複数の群に分割し、

前記攪拌暗号処理シーケンス設定ステップは、

各分割群に含まれるシングルDES暗号処理単位を各設定群内での処理順を固定とする条件の下で、各設定群のシングルDES暗号処理単位の相互入れ替えにより攪拌し、1つの攪拌暗号処理シーケンスを設定することを特徴とする請求項 11 に記載の暗号処理方法。

【請求項 15】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、

前記分割ステップは、

トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行することを特徴とする請求項11に記載の暗号処理方法。

【請求項 16】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理および乱数生成処理を含む暗号処理シーケンスであり、

前記暗号処理方法は、さらに、

乱数生成処理を3回のシングルDES処理による変換処理を含む処理として構成し、分割群のいずれかに乱数生成処理としてのトリプルDES暗号処理を設定するステップを有することを特徴とする請求項11に記載の暗号処理方法。

【請求項 17】

攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、

前記分割ステップは、

トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行し、

前記攪拌暗号処理シーケンス設定ステップは、

前記分割群の少なくともいずれかの群に、本来のオリジナル暗号処理シーケンスには不要なダミー暗号処理としてのダミーのシングルDES処理を設定し、設定するダミーのシングルDES処理数をトリプルDESに対応する3の倍数として設定する処理を含むことを特徴とする請求項11に記載の暗号処理方法。

【請求項 18】

前記暗号処理ステップは、

攪拌暗号処理シーケンスを構成する暗号処理単位の処理結果を格納するメモリに対して、いずれの暗号処理単位の処理結果であるかを識別可能な態様で処理結

果の格納を実行するステップを含むことを特徴とする請求項 1 1 に記載の暗号処理方法。

【請求項 1 9】

データ暗号処理を実行する暗号処理方法であり、

オリジナル暗号処理シーケンスを、1 以上の暗号処理単位に分割する分割ステップと、

前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とする暗号処理方法。

【請求項 2 0】

前記オリジナル暗号処理シーケンスに含まれる暗号処理単位は、シングル D E S 暗号処理であり、

前記攪拌暗号処理シーケンス設定ステップは、

前記ダミー暗号処理単位をシングル D E S 暗号処理として設定することを特徴とする請求項 1 9 に記載の暗号処理方法。

【請求項 2 1】

暗号処理をコンピュータ・システム上で実行するために記述されたコンピュータ・プログラムであって、

オリジナル暗号処理シーケンスを、1 以上の暗号処理単位から構成される複数の群に分割する分割ステップと、

前記分割ステップにおいて設定した各群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンス設定ステップにおいて設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

【請求項 22】

暗号処理をコンピュータ・システム上で実行するために記述されたコンピュータ・プログラムであって、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位に分割する分割ステップと、

前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムに関する。さらに詳細には、暗号処理を実行する例えばICモジュール等の演算回路における電力解析による暗号処理解析に対する耐性の高い暗号処理を実現する暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】

昨今、ネットワーク通信、電子商取引の発展に伴い、通信におけるセキュリティ確保が重要な問題となっている。セキュリティ確保の1つの方法が暗号技術であり、現在、様々な暗号化手法を用いた通信が実際に行なわれている。

【0003】

例えばICカード等の小型の装置中に暗号処理モジュールを埋め込み、ICカードと、データ読み取り書き込み装置としてのリーダライタとの間でデータ送受

信を行ない、認証処理、あるいは送受信データの暗号化、復号化を行なうシステムが実用化されている。

【0004】

暗号処理モジュールにおいては、例えば、平文を入力し暗号文を出力するデータ暗号化処理、あるいは暗号文を入力し平文を出力する復号化処理が実行される。これらの暗号処理は、暗号処理モジュールを構成するハードウェア、例えば半導体による電氣的な処理を含む。従って、このような半導体モジュールにおいて暗号処理が実行される際の電力消費を解析することで、暗号処理手順が解析されてしまうという恐れがある。

【0005】

例えば、IC等の演算処理装置に対する攻撃、すなわち暗号解読攻撃として、処理時間を解析することによる秘密情報を推定するTiming attack (TA)、暗号処理時の消費電力の観測により秘密情報を推定するSimple Power Analysis (SPA)、さらに、大量のデータに対する暗号処理における消費電力を測定し、それらの測定データを統計的に解析することにより秘密情報を推定するDifferential Power Analysis (DPA) 等がある。

【0006】

電力解析に対する耐性を高めるための技術については、すでいくつか提案されている。例えば、特許文献1には、中間データ制御手段を設け、暗号処理において生成される中間データを乱数によって変化させ、乱数によって消費電力をコントロールすることで、消費電力に基づく解析を困難とした構成が示されている。さらに、特許文献2、特許文献3には、暗号処理回路を構成するバスの電流検出による解析を防止する構成として、バスを転送するデータのバイト数を制御する構成を付加することで、解析を困難にする構成が示されている。

【0007】

さらに、特許文献4には、暗号処理モジュール内の演算処理と、レジスタ間のデータ移動を時間的に並列に実行させることにより、消費電力による解析を困難とした構成が示され、また、特許文献5には、メモリに対するデータ書き込み処

理の際に乱数に基づいて生成した値の書き込み処理を実行することにより、解析を困難とした構成が示されている。

【0008】

上述のように、電力解析に対する耐性を向上させようとする様々な技術が提案されている。しかし、中間データに対する乱数に基づく電力コントロールを行なう構成では、暗号処理シーケンス中のどの位置において乱数に基づく電力コントロール位置が行われているかが解明されてしまった場合、その位置以外の実質的な暗号処理シーケンス実行位置における電力解析が可能となる恐れがある。また並列処理による電力解析を困難化させようとする構成においても、暗号処理シーケンス中の特定のステップで並列処理を実行すると、並列処理の処理位置が解明されてしまうと電力解析が可能となる恐れがある。

【0009】

【特許文献1】

特開 2000-305453号公報

【特許文献2】

特開 2001-256116号公報

【特許文献3】

特開 2001-256713号公報

【特許文献4】

特開 2002-526797号公報

【特許文献5】

特開 2002-526849号公報

【0010】

【発明が解決しようとする課題】

本発明は、上記問題点に鑑みてなされたものであり、オリジナルの暗号処理シーケンスを攪拌して実行する構成において、数百～数万種類の異なる攪拌暗号処理シーケンスの設定を可能とし、これら多数の設定可能なシーケンスから選択したシーケンスを実行することにより、オリジナルの暗号処理シーケンスの持つ規則的な処理に伴う消費電力変動とは全く異なる消費電力変動を発生させ、電力解

析による暗号解析の困難性を高めることを可能とした暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0011】

【課題を解決するための手段】

本発明の第1の側面は、

データ暗号処理を実行する暗号処理装置であり、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割し、各設定群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する制御部と

、
前記制御部の設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理部と、

を有することを特徴とする暗号処理装置にある。

【0012】

さらに、本発明の暗号処理装置の一実施態様において、前記制御部は、前記分割群の少なくともいずれかの群に、前記オリジナル暗号処理シーケンスには不要なダミーの暗号処理を実行するダミー暗号処理単位を設定し、該ダミー暗号処理単位を含む複数の群の暗号処理単位の攪拌を実行して1つの攪拌暗号処理シーケンスを設定する構成であることを特徴とする。

【0013】

さらに、本発明の暗号処理装置の一実施態様において、前記制御部は、1以上の暗号処理単位から構成される複数の群への分割処理において、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、該独立実行可能なシーケンスを単位とした分割群の設定処理を実行する構成であることを特徴とする。

【0014】

さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理単位は、シングルDES暗号処理であり、前記制御部は、1以上のシングルDES暗号処理を含むオリジナル暗号処理シーケンスを1以上のシングルDES暗号処理から

構成される複数の群に分割して、各分割群に含まれるシングルDES暗号処理単位を各設定群内での処理順を固定とする条件の下で、各設定群のシングルDES暗号処理単位の相互入れ替えにより攪拌し、1つの攪拌暗号処理シーケンスを設定する構成であることを特徴とする。

【0015】

さらに、本発明の暗号処理装置の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、前記制御部は、トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行する構成であることを特徴とする。

【0016】

さらに、本発明の暗号処理装置の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理および乱数生成処理を含む暗号処理シーケンスであり、前記制御部は、乱数生成処理を3回のシングルDES処理による変換処理を含む処理として構成し、分割群のいずれかに乱数生成処理としてのトリプルDES暗号処理を設定する構成としたことを特徴とする。

【0017】

さらに、本発明の暗号処理装置の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、前記制御部は、トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行するとともに、前記分割群の少なくともいずれかの群に、本来のオリジナル暗号処理シーケンスには不要なダミー暗号処理としてのダミーのシングルDES処理を設定し、設定するダミーのシングルDES処理数をトリプルDESに対応する3の倍数として設定する構成としたことを特徴とする。

【0018】

さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理装置は、前記制御部の設定した攪拌暗号処理シーケンスを構成する暗号処理単位の処理結果を格納するメモリを有し、前記制御部は、前記メモリに対して、いずれの暗号

処理単位の処理結果であるかを識別可能な態様で処理結果の格納を実行する構成であることを特徴とする。

【0019】

さらに、本発明の第2の側面は、

データ暗号処理を実行する暗号処理装置であり、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位に分割し、前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する制御部と、

前記制御部の設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理部と、

を有することを特徴とする暗号処理装置にある。

【0020】

さらに、本発明の暗号処理装置の一実施態様において、前記オリジナル暗号処理シーケンスに含まれる暗号処理単位は、シングルDES暗号処理であり、前記制御部は、前記ダミー暗号処理単位をシングルDES暗号処理として設定する構成であることを特徴とする。

【0021】

さらに、本発明の第3の側面は、

データ暗号処理を実行する暗号処理方法であり、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割する分割ステップと、

前記分割ステップにおいて設定した各群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンス設定ステップにおいて設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とする暗号処理方法にある。

【0022】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理方法は、さらに、前記分割群の少なくともいずれかの群に、前記オリジナル暗号処理シーケンスには不要なダミーの暗号処理を実行するダミー暗号処理単位を設定するステップを含み、前記攪拌暗号処理シーケンス設定ステップは、前記ダミー暗号処理単位を含む複数群の暗号処理単位の攪拌を実行して1つの攪拌暗号処理シーケンスを設定することを特徴とする。

【0023】

さらに、本発明の暗号処理方法の一実施態様において、前記分割ステップは、1以上の暗号処理単位から構成される複数の群への分割処理において、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、該独立実行可能なシーケンスを単位とした分割群の設定処理を実行するステップであることを特徴とする。

【0024】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理単位は、シングルDES暗号処理であり、前記分割ステップは、1以上のシングルDES暗号処理を含むオリジナル暗号処理シーケンスを1以上のシングルDES暗号処理から構成される複数の群に分割し、前記攪拌暗号処理シーケンス設定ステップは、各分割群に含まれるシングルDES暗号処理単位を各設定群内での処理順を固定とする条件の下で、各設定群のシングルDES暗号処理単位の相互入れ替えにより攪拌し、1つの攪拌暗号処理シーケンスを設定することを特徴とする。

【0025】

さらに、本発明の暗号処理方法の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、前記分割ステップは、トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行することを特徴とする。

【0026】

さらに、本発明の暗号処理方法の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理および乱数生成処理を含む

暗号処理シーケンスであり、前記暗号処理方法は、さらに、乱数生成処理を3回のシングルDES処理による変換処理を含む処理として構成し、分割群のいずれかに乱数生成処理としてのトリプルDES暗号処理を設定するステップを有することを特徴とする。

【0027】

さらに、本発明の暗号処理方法の一実施態様において、攪拌対象となるオリジナル暗号処理シーケンスは、トリプルDES暗号処理を含む暗号処理シーケンスであり、前記分割ステップは、トリプルDES暗号処理を構成するシングルDES暗号処理を暗号処理単位として、1以上の暗号処理単位から構成される複数の群に分割する処理を実行し、前記攪拌暗号処理シーケンス設定ステップは、前記分割群の少なくともいずれかの群に、本来のオリジナル暗号処理シーケンスには不要なダミー暗号処理としてのダミーのシングルDES処理を設定し、設定するダミーのシングルDES処理数をトリプルDESに対応する3の倍数として設定する処理を含むことを特徴とする。

【0028】

さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、攪拌暗号処理シーケンスを構成する暗号処理単位の処理結果を格納するメモリに対して、いずれの暗号処理単位の処理結果であるかを識別可能な態様で処理結果の格納を実行するステップを含むことを特徴とする。

【0029】

さらに、本発明の第4の側面は、
データ暗号処理を実行する暗号処理方法であり、
オリジナル暗号処理シーケンスを、1以上の暗号処理単位に分割する分割ステップと、
前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、
前記攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップ

と、

を有することを特徴とする暗号処理方法にある。

【0030】

さらに、本発明の暗号処理方法の一実施態様において、前記オリジナル暗号処理シーケンスに含まれる暗号処理単位は、シングルDES暗号処理であり、前記攪拌暗号処理シーケンス設定ステップは、前記ダミー暗号処理単位をシングルDES暗号処理として設定することを特徴とする。

【0031】

さらに、本発明の第5の側面は、

暗号処理をコンピュータ・システム上で実行するために記述されたコンピュータ・プログラムであって、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割する分割ステップと、

前記分割ステップにおいて設定した各群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンス設定ステップにおいて設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【0032】

さらに、本発明の第6の側面は、

暗号処理をコンピュータ・システム上で実行するために記述されたコンピュータ・プログラムであって、

オリジナル暗号処理シーケンスを、1以上の暗号処理単位に分割する分割ステップと、

前記暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、前記ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する攪拌暗号処理シーケンス設定ステップと、

前記攪拌暗号処理シーケンスに従って、暗号処理を実行する暗号処理ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【0033】

【作用】

本発明の構成によれば、オリジナルの暗号処理シーケンスの複数群への分割およびダミーの設定により、数百～数万種類の異なる攪拌暗号処理シーケンスの設定を可能とし、これら多数の設定可能なシーケンスから選択したシーケンスを実行する構成としたので、選択された攪拌暗号処理シーケンスの実行毎に、オリジナルの暗号処理シーケンスの持つ規則的な処理に伴う消費電力変動とは全く異なる消費電力変動を発生させることが可能となり、電力解析による暗号解析の困難性を著しく高めることができる。

【0034】

さらに、本発明の構成によれば、オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割する場合に、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、独立実行可能なシーケンスを単位とした分割群の設定処理を実行するとともに、各設定群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行する構成としたので、攪拌暗号処理シーケンスを実行した場合においても必要な処理結果を確実に取得することが可能となる。

【0035】

さらに、本発明の構成によれば、乱数発生処理、あるいは設定するダミーについて、例えばオリジナル暗号処理がトリプルDESを基本とするアルゴリズムである場合、乱数生成、変換処理をトリプルDES処理によって実行する態様とし、またダミーも3の倍数に相当するシングルDESの設定としたので、全ての処理についてオリジナルのトリプルDESとの判別が困難となり、電力解析の困難性を高めることができる。

【0036】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コ

ードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0037】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づく、より詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0038】

【発明の実施の形態】

以下、本発明の暗号処理装置および暗号処理方法、並びにコンピュータ・プログラムについて、図面を参照して説明する。

【0039】

暗号処理アルゴリズムには様々なものがあるが、大きく分類すると、暗号化鍵と復号化鍵を異なる鍵、例えば公開鍵と秘密鍵として設定する公開鍵暗号方式と、暗号化鍵と復号化鍵を共通の鍵として設定する共通鍵暗号方式とに分類される。

【0040】

共通鍵暗号方式の1つに共通鍵をベースとして複数の鍵を生成して、生成した複数の鍵を用いて暗号処理を繰り返し実行する方式がある。このような鍵生成方式を適用したアルゴリズムの代表的なものが共通鍵ブロック暗号方式である。

【0041】

共通鍵ブロック暗号のアルゴリズムは、主として、入力データの変換を実行するラウンド関数部と、ラウンド関数部の各ラウンドで適用する鍵を生成する鍵スケジュール部とに分けることができる。ラウンド関数部の各ラウンドで適用する鍵（副鍵）は、1つの主鍵に基づいて、鍵スケジュール部に入力されて生成され、各ラウンド関数部で適用される。この共通鍵暗号方式の代表的な方式に米国連

邦標準暗号方式としてのDES (Data Encryption Standard) がある。

【0042】

DES暗号処理の基本構造について、図を参照して説明する。DES暗号処理は、変換関数の単純な繰り返しにより、平文を暗号文に変換する構造を持つ。図1にDES暗号処理の基本構成を示す。入力データの変換を実行するラウンド関数部110と、ラウンド関数部の各ラウンドで適用する鍵を生成する鍵スケジュール部120とによって構成される。

【0043】

ラウンド関数部110において、平文(64ビット)は、まず、初期置換部111において、L, R各32ビットに分割され、分割されたL, R32ビットが、第1段変換部112に入力され、鍵スケジュール部120の第1段鍵生成部122から入力する鍵K(1)に基づいて変換処理がなされる。変換処理結果は、次段の第2段変換部113に入力される。

【0044】

鍵スケジュール部120においては、まず、選択置換部121により入力主鍵(64ビット)のパリティ8ビットが取り除かれ、残り56ビットの入れ替え処理が実行されて第1段鍵生成部122に入力される。第1段鍵生成部122では、入力ビット列のシフト処理およびパリティビットの除去等が実行され、48ビットの副鍵K(1)を生成し、生成した副鍵K(1)をラウンド関数部110の第1段変換部112に出力する。第1段鍵生成部122では、シフト処理による上位ビット列(28ビット)と下位ビット列(28ビット)とを下段の第2段鍵生成部123に出力する。

【0045】

ラウンド関数部は、16段の変換部を有し、それぞれ前段の変換部の出力を入力として鍵スケジュール部120から入力する鍵を適用した変換処理を実行し、変換結果を後段の変換部に出力する。16段の変換部で変換された出力が逆置換部114に入力され、初期置換部111の逆置換処理が実行されて、暗号文として出力される。

【0046】

ラウンド関数部 110 の各ラウンドを構成する変換部の構成を図 2 に示す。図 2 に示すように、変換部は、前段 ($n-1$ 段) の変換部から 2 つの入力、 $L(n-1)$ 、 $R(n-1)$ を入力し、鍵スケジュール部から鍵 ($k(n)$) を入力する。F 関数部 151 において、鍵スケジュール部から入力する鍵 ($k(n)$) を用いて、前段変換部から入力するビット列 ($R(n-1)$) の変換処理がなされ、変換結果が、前段変換部から入力する残りのビット列 ($L(n-1)$) と排他論理和が実行されて、次段の変換部の出力 $R(n)$ が生成される。次段の変換部には、 $R(n-1)$ を $L(n)$ としたビット列と、上述の F 関数および排他論理和演算により生成された $R(n)$ が入力され同様の処理が繰り返される。

【0047】

F 関数の構成を図 3 に示す。F 関数は、非線形処理を実行する複数の S ボックス (S b o x) を有する。ラウンド関数部の前段からの入力値 $R(n-1)$ は置換部 171 によって 48 ビットに拡大され、さらに鍵スケジュール部から入力する鍵 (48 ビット) と排他論理和が実行され、その出力が 6 ビットずつ非線形変換処理を実行する複数の S ボックス 181-1~8 に入力される。各 S ボックスでは、例えば変換テーブルを適用した 6 ビットから 4 ビットへの非線形変換処理が実行される。

【0048】

S ボックス 181-1~8 からの出力ビット $4 \times 8 = 32$ ビットは、置換部 172 に入力されて、ビット位置の入れ替え処理がなされ、F 関数出力 32 ビットを生成して出力する。

【0049】

図 1~3 を参照して説明したように複数段 (16 段) の変換処理によって DES 暗号処理が実行される。この DES 暗号処理をさらに暗号強度を高めるため複数繰り返し実行する構成、例えば 3 回の DES 暗号処理を実行するトリプル DES 暗号処理が様々な分野、例えばインターネットを介したデータ通信機器間の相互認証処理や、IC カードとリーダーライター間の相互認証処理等に適用する暗号処理として多く採用されている。なお、トリプル DES 暗号処理と区別するため、回の DES 暗号処理をシングル DES 暗号処理と呼ぶ。

【0050】

トリプルDES (Triple DES) 暗号処理構成は、図4に示すように、図1～3を参照して説明したDES暗号処理を3回繰り返して実行することにより、平文から暗号文を生成する。シングルDES暗号処理部185、186、187のそれぞれが上述した16段のラウンド関数部を持ち、Sボックスを持つF関数による処理を16回繰り返す。

【0051】

通常、トリプルDES暗号処理では、最初のシングルDES暗号処理部185と、最後のDES暗号処理部187においては同じ主鍵(K1)を適用し、中間のDES暗号処理部186には異なる主鍵(K2)を適用する。このように、DES暗号処理を複数回繰り返して実行することで、暗号強度を向上させることができる。

【0052】

このトリプルDES暗号処理を適用した処理例として、インターネットを介したデータ通信機器間、あるいはICカードとリーダライタ間で実行される相互認証処理のシーケンスを図5に示す。

【0053】

図5には、右側にICカード、左側にICカードとのデータ通信を実行するリーダライタを示す。それぞれのデバイスは、上述のトリプルDES暗号処理を実行可能な暗号処理モジュールを格納し、相互に接触または非接触でのデータ通信が可能な構成を持つ。

【0054】

図5に示すDES共通鍵暗号方式による相互認証処理手順について説明する。まず、ステップS101において、リーダライタが乱数[Rr]を入力とし、リーダライタとICカードが共通に所有する鍵[KeyA]を用いてトリプルDES暗号処理(T-DES)を実行し、暗号化データ[A1]を生成し、生成した暗号化データ[A1]をICカードに送信する。なお、前述したように、トリプルDES暗号処理には、2つの異なる鍵が適用され、上述の鍵[KeyA]は、トリプルDES暗号処理に適用する2つの異なる鍵の組合わせを示す。

【0055】

暗号化データ [A1] を受信した IC カードは、ステップ S102 において、共通に所有する鍵 [Key A] を用いて受信した暗号化データ [A1] をトリプル DES により復号し、復号データ [A1__1] を得る。なお、復号処理においてもトリプル DES 暗号処理構成が適用される。すなわち、トリプル DES 暗号処理部に暗号文を入力し平文を出力する。さらに IC カードは、復号データ [A1__1] を、やはり、リーダライタと IC カードが共通に所有する鍵 [Key B] を用いてトリプル DES 暗号処理を実行して、暗号化データ [B1] を生成する。

【0056】

さらに、IC カードは、ステップ S103 において、乱数 [Rc] を作り、生成乱数 [Rc] を、鍵 [Key B] を用いて、トリプル DES 暗号処理を実行して暗号化データ [B2] を生成する。IC カードは、生成した暗号化データ [B1] と、暗号化データ [B2] とをリーダライタに送信する。

【0057】

リーダライタは、IC カードから暗号化データ [B1] と、暗号化データ [B2] とを受信すると、ステップ S104 において、暗号化データ [B1] を鍵 [Key B] にて復号し、復号データ [B1__1] を得る。ここで、復号データ [B1__1] が先に生成した乱数 Rr と等しいか否かを検証する。等しい場合には、リーダライタは、IC カードが正当な共通鍵を持つデバイスであると認証する。

【0058】

さらに、リーダライタは、ステップ S105 において、暗号化データ [B2] を鍵 [Key B] にて復号し、復号データ [B2__1] を得る。さらに、復号データ [B2__1] に対して、鍵 [Key A] を適用してトリプル DES 暗号処理を実行して暗号化データ [A2] を得る。この暗号化データ [A2] を IC カードに送信する。

【0059】

IC カードは、リーダライタから暗号化データ [A2] を受信すると、ステッ

プS106において、暗号化データ [A2] を、鍵 [KeyA] を適用して復号し、復号データ [A2__1] を取得する。ここで、復号データ [A2__1] が先に生成した乱数Rcと等しいか否かを検証する。等しい場合には、ICカードは、リーダライタが正当な共通鍵を持つデバイスであると認証する。ICカードは、復号データ [A2__1] をリーダ/ライタに送信する。

【0060】

以上の処理により、ICカード、リーダライタがそれぞれ同一の共通鍵を持つ正当なデバイスであることが証明される。相互にデータ通信を行なう場合は、例えばICカードの生成乱数Rc (=A2__1) をセッション鍵として通信データの暗号化、復号化用鍵として適用したデータ通信を行なう。

【0061】

上述の共通鍵認証シーケンスにおいて、例えばICカードの処理ステップS102とS103の処理シーケンスを暗号処理時の消費電力の観測により秘密情報を推定するSimple Power Analysis (SPA)、あるいは、大量のデータに対する暗号処理における消費電力を測定し、それらの測定データを統計的に解析することにより秘密情報を推定するDifferential Power Analysis (DPA) 等を適用すると、暗号処理に適用する鍵データ列が漏洩する可能性がある。

【0062】

上述の共通鍵認証シーケンスにおけるICカードの処理ステップS102とS103の処理シーケンスをICカード内の暗号処理モジュールで実行する場合のシーケンスについて、図6を参照して説明する。ICカードの処理シーケンスは、図6(a)に示す処理となる。

【0063】

すなわち、ステップS102とステップS103において、

(1) 暗号化データ [A1] のトリプルDESによる復号処理による復号データ [A1__1] の取得。

(2) 復号データ [A1__1] のトリプルDES暗号処理による暗号化データ [B1] の生成。

(3) 乱数 [R c] の生成処理。

(4) 乱数 [R c] を入力として、トリプルDES暗号処理を実行して暗号化データ [B 2] を生成。

【0064】

以上の(1)～(4)の処理がシーケンシャルに行なわれる。具体的には、図6(b)に示すように、時間軸 t に沿って、(1)トリプルDES、(2)トリプルDES、(3)乱数生成、(4)トリプルDESが、順次実行されることになる。これらの処理を実行するICカードの電力消費の変動シーケンスは、DES暗号処理シーケンス(1)～(4)に対応したものとなる。

【0065】

DES暗号処理は、前述したように、ラウンド関数部において、複数段のF関数を繰り返し実行するものである。F関数を構成する非線形変換処理実行部としてのSボックスを適用したデータ変換実行時における電力変動を解析することで、データ変換処理の解析が可能となる場合がある。従って、データシーケンスが、図6(b)のように実行されることが把握されると、各DES暗号処理におけるSボックスを適用した変換タイミングも容易に推測可能であり、様々な入力データに基づいて、そのタイミングにおける消費電力変動を計測することが可能となり、不正者による暗号解析を許容することになる。

【0066】

本発明の暗号処理装置、暗号処理方法は、図6に示すような規則的な処理シーケンスを攪拌することにより、暗号解析に対する耐性を高めた構成を提供するものである。

【0067】

図7を参照して本発明の暗号処理シーケンスの構成について説明する。本発明の暗号処理装置および方法においては、従来の規則的な暗号処理シーケンスに対して、以下のような処理を行ないオリジナル暗号処理シーケンスの攪拌を実行し、攪拌暗号処理シーケンスを設定する。

【0068】

(a) 乱数 (R c) の拡張

シングルDES暗号処理を3回実行して生成乱数の変換処理を行なう。どの乱数を実際の処理に適用する乱数とするかは任意である。シすなわち、初期設定の乱数でもよいし、DES暗号処理によって変換された値でもよい。シングルDES暗号処理を3回行うのは、解析者から見た際に乱数の発生もトリプルDES (Triple-DES) の処理であると認識させ、他のトリプルDES (Triple-DES) 処理との判別を困難にするためである。

(b) ダミーの追加

一連の処理の最後にn個のダミーのDES暗号処理を挿入し、処理全体として解析に意味があるデータか否かの判別を困難にさせる。なお、ダミーの追加は乱数の拡張と同様に3の倍数にする。理由は、乱数と同じく各処理をTriple-DESに見せるため

【0069】

図7に示すように、共通鍵認証シーケンスにおけるICカードの処理ステップS102とS103の処理シーケンスを2つの群、X群とY群に分割する。

【0070】

X群は、

(1) 暗号化データ [A1] のトリプルDESによる復号処理による復号データ [A1__1] の取得。

(2) 復号データ [A1__1] のトリプルDES暗号処理による暗号化データ [B1] の生成。

【0071】

Y群は、

(3) 乱数 [Rc] の生成処理。

(4) 乱数 [Rc] を入力として、トリプルDES暗号処理を実行して暗号化データ [B2] を生成。

(5) n個のダミーのシングルDES処理実行。

により構成する。

【0072】

上述のように、処理(1)～(4)に(5)のダミーによるシングルDES処

理を付加し、(1)、(2)をX群、(3)、(4)、(5)をY群として区分した後、これらの処理シーケンスを攪拌する。

【0073】

本発明の暗号処理装置では、1以上の暗号処理単位（例えばシングルDES）から構成されるオリジナル暗号処理シーケンスを複数の群へ分割する場合、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、独立実行可能なシーケンスを単位とした分割群の設定処理を実行し、必要に応じて設定群のいずれかにダミーの設定を行なう。上述の例では、(1)、(2)の処理は1つの独立して実行可能なシーケンスであり、(3)、(4)の処理は、もう1つの独立して実行可能なシーケンスである。

【0074】

攪拌暗号処理シーケンスを生成するための攪拌処理について、図8を参照して説明する。図8には、X群の(1) [A1__1]の生成において実行するトリプルDESを構成するシングルDESをX1, X2, X3として示し、(2) [B1]の生成において実行するトリプルDESを構成するシングルDESをX4, X5, X6として示している。

【0075】

また、Y群の(3) [Rc]の生成において実行するトリプルDESを構成するシングルDESをY1, Y2, Y3として示し、(4) [B2]の生成において実行するトリプルDESを構成するシングルDESをY4, Y5, Y6として示し、(5) n個のダミーにおいて実行するシングルDESをY7, Y8...Y6+nとして示している。

【0076】

これらの各DES暗号処理を順番を入れ替えて実行する。ただし、例えばX群においては、X1の後にX2を実行し、その後にX3、X4、X5、X6と実行することが必要であるため、このX1～X6の処理順序の入れ替えは行なわない。Y群においても、Y1の後にY2を実行し、その後にY3、Y4、Y5、Y6と実行することが必要であるため、このY1～Y6の処理順序の入れ替えは行なわない。

【0077】

本発明の暗号処理装置では、オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割するとともに、各設定群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定する。

【0078】

上記条件の下、X群、Y群を構成するシングルDESの処理単位X1～X6と、Y1～Y6+nとの処理順番を攪拌した場合の組み合わせ数は、以下のように計算される。

【0079】

まず、図8(A)に示すように、X群のX1～X6の前後および各間にY群を挿入する処理態様が複数ある。例えばY群を1固まりにして、図8(A)に示すX群のa1～a7の位置に挿入する場合の態様としては、 7C_1 通り、すなわち7通りとなる。また、Y群を2つに分割して図8(A)に示すX群のa1～a7の位置に挿入する場合の態様としては、 7C_2 通り、すなわち21通りとなる。以下、Y群は6+nまで分割可能であり、その場合は、 ${}^7C_{6+n}$ 通りの組み合わせがある。

【0080】

さらに、図8(B)に示すように、X群に挿入するY群の分割位置の設定態様も分割数に応じて多数の組み合わせが可能である。すなわち、Y群は、図8(B)に示すようにb1～b5+nのいずれかで分割可能である。分割数0の場合、すなわちY群を1固まりにして、X群のa1～a7の位置のいずれかに挿入する場合のY群の分割態様は、 ${}^{5+n}C_0$ 通り、すなわち1通りであるが、分割数1の場合、すなわちY群を2つにするY群の分割態様は、 ${}^{5+n}C_1$ 通りとなる。以下、Y群の分割数は5+nまで設定可能であり、この場合、すなわちY群を5+nに分割する場合のY群の分割態様は、 ${}^{5+n}C_{5+n}=1$ 通りとなる。このようにY群の分割数に応じてその組み合わせ数が決定される。

【0081】

さらに、図8(C)に示すように、6+n個のY群の中に、実質的な暗号処理

シーケンス、すなわちオリジナル暗号処理シーケンスに含まれるシングルDES処理としてのY1～Y6を配列する組み合わせ数が ${}_{6+n}C_6$ 通りとなる。

【0082】

このように、(A)、(B)、(C)の各々についての組合せ数を考慮すると、トータルとしての組み合わせ数の総計は、下式に示す計算の総数として求められる。

【0083】

【数1】

$${}^7C_1 \times {}^{5+n}C_0 \times {}^{6+n}C_6$$

$${}^7C_2 \times {}^{5+n}C_1 \times {}^{6+n}C_6$$

...

$${}^7C_{6+n} \times {}^{5+n}C_{5+n} \times {}^{6+n}C_6$$

【0084】

図9を参照して、上記式の説明をする。図9に示す計算式中(A)の部分は、図8(A)の組み合わせ数に相当する計算部分であり、X群のX1～X6の前後および各間にY群を挿入する処理態様の組み合わせ数の計算部分である。図9に示す計算式中(B)の部分は、図8(B)の組み合わせ数に相当する計算部分であり、X群に挿入するY群の分割位置の組み合わせ数の計算部分である。図9に示す計算式中(C)の部分は、図8(C)の組み合わせ数に相当する計算部分であり6+n個のY群の中に、実質的な暗号処理シーケンスに必要となるシングルDES処理としてのY1～Y6を配列する組み合わせ数、すなわち、 ${}_{6+n}C_6$ の計算部分である。

【0085】

例えば、図9の最上段の行は、X群の挿入位置を1つとして、Y群の分割数を0とした場合の組み合わせ数を計算し、次の行は、X群の挿入位置を2つとして、Y群の分割数を1つ、すなわち、2つにY群を分割してX群のいずれかに挿入する場合の組み合わせ数を計算している。最下段の行は、X群の挿入位置を7つ(Max)として、Y群の分割数を5+n(Max)とした場合の組み合わせ数を計算している。

【0086】

これら各行の計算値の総和が、X群のX1～X6、Y群のY1～Y6の処理順序を固定とした条件の下で、X群、Y群を構成するシングルDESの処理単位X1～X6と、Y1～Y6+nとの処理順番を変更する組み合わせ数となる。

【0087】

具体的な計算例について図10を参照して説明する。図10(a)は、X群X1～X6、Y群Y1～Y6に、追加ダミー数：n=0として設定した場合の組み合わせ総数を計算したものであり、その総数は942通りとなる。

【0088】

図10(b)は、X群X1～X6、Y群Y1～Y6に、追加ダミー数：n=3として設定した場合の組み合わせ総数を計算したものであり、その総数は420420通りとなる。さらに、ダミー数を増加させることにより、組み合わせ数は加速度的に増大することになる。

【0089】

本発明の暗号処理装置、暗号処理方法では、上述のように、実行すべきオリジナル暗号処理シーケンスを複数の群に分割し、それらの分割群における暗号処理単位（例えばシングルDES）を所定条件、例えば各群内のシーケンスは一定とする等の所定条件の下に攪拌し、攪拌暗号処理シーケンスを設定し設定した攪拌暗号処理シーケンスに従って暗号処理を実行する。

【0090】

従って、消費電力は、攪拌暗号処理シーケンスに応じたものとなり、前述したように規則的なシーケンスに従ったものとはならず、図5に示すICカード側の処理ステップS102とステップS103において実行される処理内のDES暗号処理のどの部分が実行中であるかを外部からの消費電力のモニタによって推察することは非常に困難となる。

【0091】

図10の具体的な数値からも明らかなように、ダミーを用いない場合であっても処理シーケンスの設定態様は、942通りであり、処理開始時にシーケンスを設定して処理を実行すれば、処理毎にシーケンスが異なることになり、外部からの

電力モニタによる暗号解析は極めて困難となる。さらに、ダミーによる処理を加えることで、図10に示すように、設定可能なシーケンス数は飛躍的に増大し、同一のシーケンスが繰り返される確率は極めて低くなる。従って、外部からの電力モニタによる暗号解析の可能性を著しく低減することが可能となる。

【0092】

なお、上述した実施例では、図5に示す認証シーケンスにおけるICカード側の処理ステップS102、S103を例として説明したが、上述のシーケンス攪拌処理は、その他の処理、例えば図5におけるリーダライタの処理ステップS104とステップS105についても同様に適用可能である。例えばステップS104の処理をX群とし、ステップS105の処理をY群として設定し、必要に応じて少なくともいずれかの群にダミー処理にむよるシングルDES処理を設定し、上述と同様の各暗号処理単位（シングルDES）の順番を入れ替える攪拌処理により、処理シーケンスを設定することが可能である。

【0093】

また、上述した実施例では、DES暗号処理を実行する構成例について説明したが、暗号処理は、DESに限らず、他の暗号処理アルゴリズムを実行する構成においても、上述と同様の処理シーケンスの攪拌により解析を困難とすることが可能である。

【0094】

様々な暗号処理アルゴリズムにおいて、例えばシングルDES等と同様の暗号処理単位を持つアルゴリズムでは、その暗号処理単位を、独立に実行可能な複数の群に分割し、必要に応じてダミーの処理単位を付加して、結果出力が可能なシーケンスを維持することを条件として、複数群の個々の処理単位の順番を入れ替える攪拌処理を実行する。このようにして設定された攪拌後の処理シーケンスに従って暗号処理を実行することで、外部からの電力解析を困難化することができる。

【0095】

また、上述した実施例では、X群、Y群の2つの群に分割する処理例を説明したが、実行すべきオリジナル暗号処理シーケンス中に独立して実行可能な暗号処

理シーケンスが3つ以上存在する場合は、3以上の群に分割して、必要に応じて各群少なくともいずれかにダミーを設定し、各分割群内の処理シーケンスを維持するなどの所定条件の下に暗号処理単位を攪拌し、攪拌した処理シーケンスを設定して暗号処理を実行する構成とすることが可能である。

【0096】

上述の暗号処理シーケンスの設定、および設定した暗号処理シーケンスを実行するデバイスとしてのICモジュール300の構成例を図11に示す。上述の処理は、例えばPC、ICカード、リーダライタ、その他、様々な情報処理装置において実行可能であり、図11に示すICモジュール300は、これら様々な機器に構成することが可能である。

【0097】

図11に示すCPU(Central processing Unit)301は、暗号処理の開始や、終了、データの送受信の制御、各構成部間のデータ転送制御、その他の各種プログラムを実行するプロセッサである。メモリ302は、CPU301が実行するプログラム、あるいは演算パラメータとしての固定データを格納するROM(Read-Only-Memory)、CPU301の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用されるRAM(Random Access Memory)等からなる。また、メモリ302は暗号処理に必要な鍵データ等の格納領域として使用可能である。データ等の格納領域は、耐タンパ構造を持つメモリとして構成されることが好ましい。

【0098】

暗号処理手部303は、例えば上述したトリプルDESに従った暗号処理、復号処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをROMに格納し、CPU301がROM格納プログラムを読み出して実行するように構成してもよい。

【0099】

乱数発生器304は、暗号処理に必要な乱数の発生処理を実行する。発生した乱数を例えばDES暗号処理によって変換する場合には、発生乱数を暗号処

理部 303 に入力し暗号処理を実行する。

【0100】

処理制御部 305 は、上述した処理において処理シーケンスの設定、すなわち、X 群、Y 群等、複数の群の設定処理、競った低した処理群に対するダミーの設定、ダミーの暗号処理（例えばシングル DES）を実行する場合のダミー暗号処理に対する入力値設定処理等を実行する。

【0101】

なお、ここでは、理解を容易にするため、処理制御部 305 を、本発明の特徴的な処理を実行する要素として独立して示したが、処理制御部 305 の上述の処理は、CPU 301、あるいは暗号処理部 303 内の制御部において実行する構成とすることも可能であり、上述の処理制御部を独立に構成することは必須ではない。

【0102】

次に、図 12、図 13 のフローチャートを参照して、本発明の暗号処理装置における暗号処理のシーケンス設定、および暗号処理の実行手順について説明する。

【0103】

図 12 のフローに示す各ステップ毎の処理について説明する。まず、暗号処理を実行する機器、例えば IC カード、リーダライタ、PC 等の機器は、ステップ S301 においてオリジナル暗号処理シーケンスを複数群に分割する。この複数群への分割は、上述した実施例における X 群、および Y 群への分割に相当する。群への分割要件は、それぞれの群の暗号処理が独立に実行可能なシーケンスとして設定されていることである。具体的には、図 5 に示す IC カードにおけるステップ S102 の暗号処理シーケンスと、ステップ S103 における暗号処理シーケンスのように、それぞれ独立に実行可能なシーケンスは個別の群として設定可能となる。リーダライタのステップ S104 と、ステップ S105 のシーケンスも個別の群として設定できる。なお、3 つ以上の独立シーケンスがあれば 3 つ以上の群に分割可能である。

【0104】

図12のフローにおけるステップS301において複数群への分割が実行されると、ステップS302において分割群のいずれかの群にダミーを設定する。これは図7、図8に示すY群のn個のダミーの設定処理である。なお、ダミーの設定は任意である。ダミーを用いない場合でも、先に図10を参照して説明したように、十分なシーケンス攪拌が可能である場合もあり、このように十分な攪拌が可能である場合には、ダミーを付加しない構成としてもよい。

【0105】

ステップS303において、分割群を所定条件下で、攪拌して、攪拌暗号処理シーケンスを設定する。所定条件とは、例えば、各個別群の中の暗号処理単位（例えばシングルDES）の処理順序の入れ替えは行なわない等の条件である。

【0106】

設定される攪拌暗号処理シーケンスは、例えば、図10の(b)の例のX群X1～X6、Y群Y1～Y6に、追加ダミー数：n=3として設定した場合、420420通りのシーケンスから選択された1つのシーケンスとなる。このシーケンスの選択は、例えば暗号処理装置の制御部がランダムに選択する。

【0107】

実行する攪拌暗号処理シーケンスの選択が終了すると、ステップS304において、設定されたシーケンスに従って、暗号処理を実行する。暗号処理の実行詳細を図13のフローチャートを参照して説明する。

【0108】

図13のフローは、攪拌暗号処理シーケンスを構成する各処理単位、すなわち上述の実施例では、図7、図8に示す1つの円に対応するシングルDESの処理における処理手順を示している。ステップS501において、処理単位（例えばシングルDES）に入力する値をメモリから取得し、ステップS502において、入力値に基づく暗号処理（例えばシングルDES）を実行する。

【0109】

メモリから取得する値は、前段の結果の入力な処理である場合には、前段の処理結果をメモリから取得する。例えば、図8において、X群のX2の処理においては、X1の処理結果を入力することが必要となる。この場合には、メモリから

前段の出力結果を取得し、入力値とする。

【0110】

ステップS502において、暗号処理単位の処理が実行されると、ステップS503において、結果をメモリに格納する。格納する場合は、どの処理単位のデータであるかを判別可能な状態で格納する。例えば図8において、X群のX2の処理を実行した場合は、X2の処理結果であることを判別可能な態様で格納する。こうすることで、X3の処理が実行される際、X3の入力値を誤りなくメモリから取得可能となる。

【0111】

ステップS504において、実行した処理単位が、攪拌暗号処理シーケンスの最終処理単位であるか否かを判定し、Noである場合には、ステップS501に戻り、メモリから入力値を取り出して暗号処理を実行するシーケンスを繰り返す。

【0112】

ステップS504において、実行した処理単位が、攪拌暗号処理シーケンスの最終処理単位であると判定された場合は、ステップS505に進み、メモリに格納された値の中から、ダミーに基づく処理結果を除く、各群の実際に必要となるオリジナル暗号処理シーケンスの最終処理結果をメモリに保存あるいは必要に応じて出力する。図7または図8に示す例では、X群における処理単位X6の処理結果と、Y群における処理単位Y6の処理結果が、メモリに対する保存あるいは出力データとされる。これは、図5に示す例においては、ステップS102の結果[B1]と、ステップS103の結果[B2]に相当する値である。

【0113】

上述のようにオリジナル暗号処理シーケンスを複数群に分割し、必要に応じてダミーを設定し、攪拌暗号処理シーケンスを設定後に暗号処理を実行することで、オリジナル暗号処理シーケンスに対応した規則的な処理シーケンスが実行されることがなくなり、電力解析による暗号処理解析の困難性が高められる。

【0114】

なお、上述の実施例では、オリジナル暗号処理シーケンスを複数群に分割する

ことを前提として説明したが、独立して実行可能なシーケンスが複数存在しない場合には、複数群への分割を実行せず、ダミーの追加のみを実行して、追加したダミーと、オリジナル暗号処理シーケンスの処理単位とに基づく攪拌を実行する構成としてもよい。

【0115】

すなわち、オリジナル暗号処理シーケンスを、暗号処理単位に分割し、暗号処理単位に相当する処理を実行するダミー暗号処理単位を付加し、オリジナル暗号処理シーケンス中に含まれるオリジナル暗号処理単位と、ダミー暗号処理単位の処理順の攪拌を実行して攪拌暗号処理シーケンスを設定し、設定した攪拌暗号処理シーケンスに従って、暗号処理を実行する構成としてもよい。この場合、例えば、オリジナル暗号処理シーケンスに含まれる暗号処理単位が、シングルDES暗号処理である場合は、ダミー暗号処理単位もシングルDES暗号処理として設定する。

【0116】

次に、暗号処理ICモジュールを持つPC、ポータブルデバイス、リーダライタ、ICカード等の機器の構成例について、図14を参照して説明する。図11では、上述の処理を実行するための最低限の構成要素として、暗号処理ICモジュールのみの構成を示したが、図14に、データ入出力可能な通信部、その他の記憶部、入力部、出力部等を備え、上述の暗号処理シーケンスの設定、実行、さらにデータ入出力可能な構成を含む情報処理装置の一般的構成について説明する。

【0117】

上述の実施例で述べた一連の処理は、ハードウェア、ソフトウェアの組み合わせにより行うことができる。即ち、汎用のコンピュータや、マイクロコンピュータにプログラムを実行させることにより行う構成とすることが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、例えば汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図14は、上述した一連の処理を実行するプログラムをインストールして実行可能なコンピュータの一実施形態としての構成例を示している。

【0118】

図14に示すシステム構成例は1つの例であり、本発明の処理を実行するシステムは、ここに示すすべての機能を必ずしも備えることが要求されるものではない。図14に示すCPU(Central processing Unit)501は、上述したアルゴリズムに従ったプログラムやその他の各種アプリケーションプログラム、OS(Operating System)を実行するプロセッサである。この例では、図11に示す処理制御部の処理もCPU501の制御の下に実行される。

【0119】

ROM(Read-Only-Memory)502は、CPU501が実行するプログラム、あるいは演算パラメータとしての固定データを格納する。RAM(Random Access Memory)503は、CPU501の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用される。

【0120】

HDD504はハードディスクの制御を実行し、ハードディスクに対する各種データ、プログラムの格納処理および読み出し処理を実行する。暗号処理手段505は、データの暗号処理、復号処理、乱数発生処理等を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをROM502に格納し、CPU501がROM格納プログラムを読み出して実行するように構成してもよい。メモリ(セキュアモジュール)506は例えば耐タンパ構造を持つメモリとして構成され、暗号処理に必要な鍵データ等の格納領域として使用可能である。なお、これらのデータは、他のメモリ領域、記憶媒体に格納することも可能である。

【0121】

バス521はPCI(Peripheral Component Internet/Interface)バス等により構成され、各モジュール、入出力インタフェース122を介した各入力装置とのデータ転送を可能にしている。

【0122】

入力部 511 は、例えばキーボード、ポインティングデバイス、あるいはその他のデータ入力手段によって構成され、CPU 501 に各種のデータあるいはコマンドを入力する。出力部 512 は、例えば CRT、液晶ディスプレイ等であり、各種情報をテキストまたはイメージ等により表示する。

【0123】

通信部 513 はシステムの接続したエンティティ、例えば暗号データの通信エンティティ（例えばリーダライタ）との通信処理を実行し、CPU 501 の制御の下に、各記憶部から供給されたデータ、あるいは CPU 501 によって処理されたデータ、暗号化されたデータ等を送信したり、他エンティティからのデータを受信する処理を実行する。

【0124】

ドライブ 514 は、フレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 515 の記録再生を実行するドライブであり、各リムーバブル記録媒体 515 からのプログラムまたはデータ再生、リムーバブル記録媒体 515 に対するプログラムまたはデータ格納を実行する。

【0125】

各記憶媒体に記録されたプログラムまたはデータを読み出して CPU 501 において実行または処理を行なう場合は、読み出したプログラム、データはインタフェース 522、バス 521 を介して例えば接続されている RAM 503 に供給される。

【0126】

先にフロー図を参照した処理を実行するためのプログラムは例えば ROM 502 に格納されて CPU 501 によって処理されるか、あるいはハードディスクに格納され、ハードディスクから読み出されて CPU 501 により実行される。

【0127】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得

ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0128】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【0129】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory) に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0130】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

【0131】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的あるいは個別に実行されてもよい。

【0132】**【発明の効果】**

以上、説明してきたように、本発明の構成によれば、オリジナルの暗号処理シーケンスの複数群への分割およびダミーの設定により、数百～数万種類の異なる攪拌暗号処理シーケンスの設定を可能とし、これら多数の設定可能なシーケンスから選択したシーケンスを実行する構成としたので、選択された攪拌暗号処理シーケンスの実行毎に、オリジナルの暗号処理シーケンスの持つ規則的な処理に伴う消費電力変動とは全く異なる消費電力変動を発生させることが可能となり、電力解析による暗号解析の困難性を著しく高めることができる。

【0133】

さらに、本発明の構成によれば、オリジナル暗号処理シーケンスを、1以上の暗号処理単位から構成される複数の群に分割する場合に、分割対象となるオリジナル暗号処理シーケンス中、独立して実行可能なシーケンス群を判別し、独立実行可能なシーケンスを単位とした分割群の設定処理を実行するとともに、各設定群内の暗号処理単位の処理順を固定とする条件の下で暗号処理単位の処理順の攪拌を実行する構成としたので、攪拌暗号処理シーケンスを実行した場合においても必要な処理結果を確実に取得することが可能となる。

【0134】

さらに、本発明の構成によれば、乱数発生処理、あるいは設定するダミーについて、例えばオリジナル暗号処理がトリプルDESを基本とするアルゴリズムである場合、乱数生成、変換処理をトリプルDES処理によって実行する態様とし、またダミーも3の倍数に相当するシングルDESの設定としたので、全ての処理についてオリジナルのトリプルDESとの判別が困難となり、電力解析の困難性を高めることができる。

【図面の簡単な説明】**【図1】**

DES暗号処理アルゴリズムについて説明する図である。

【図2】

DES暗号処理アルゴリズムにおけるラウンド関数部の構成について説明する図

である。

【図 3】

DES 暗号処理アルゴリズムにおけるラウンド関数部内の S ボックス構成について説明する図である。

【図 4】

トリプル DES 暗号処理構成について説明する図である。

【図 5】

共通鍵方式の相互認証処理シーケンスについて説明する図である。

【図 6】

共通鍵方式の相互認証処理シーケンスにおける IC カード側の詳細処理シーケンスを説明する図である。

【図 7】

本発明の暗号処理における分割群の設定処理について説明する図である。

【図 8】

本発明の暗号処理における分割群の設定および攪拌暗号処理シーケンスの設定について説明する図である。

【図 9】

本発明の暗号処理における攪拌暗号処理シーケンスの設定態様数の計算について説明する図である。

【図 10】

本発明の暗号処理における攪拌暗号処理シーケンスの設定態様数の計算の具体例について説明する図である。

【図 11】

本発明の暗号処理を実行する IC モジュールの構成例を説明するブロック図である。

【図 12】

本発明の暗号処理の手順を説明するフローチャートである。

【図 13】

本発明の暗号処理の手順を説明するフローチャートである。

【図 14】

本発明の暗号処理を実行する情報処理装置構成例を示す図である。

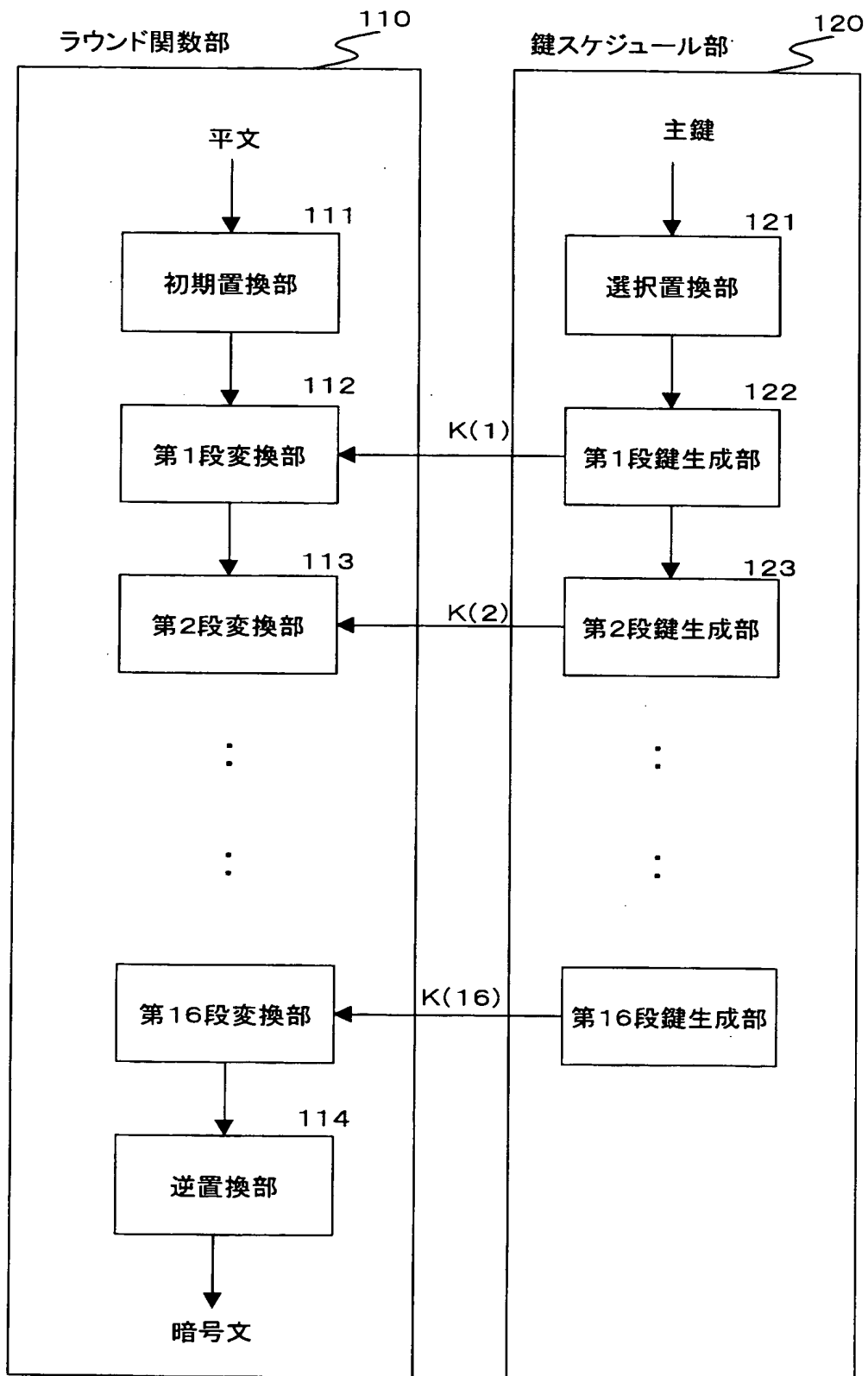
【符号の説明】

- 110 ラウンド関数部
- 111 初期置換部
- 112 第1変換部
- 113 第2変換部
- 114 逆置換部
- 120 鍵スケジュール部
- 121 選択置換部
- 122 第1鍵生成部
- 123 第2鍵生成部
- 151 F関数部
- 171 置換部
- 172 置換部
- 181 Sボックス
- 185～187 DES暗号処理部
- 300 ICモジュール
- 301 CPU
- 302 メモリ
- 303 暗号処理部
- 304 乱数発生器
- 305 処理制御部
- 501 CPU
- 502 ROM
- 503 RAM
- 504 HDD
- 505 暗号処理手段
- 506 メモリ

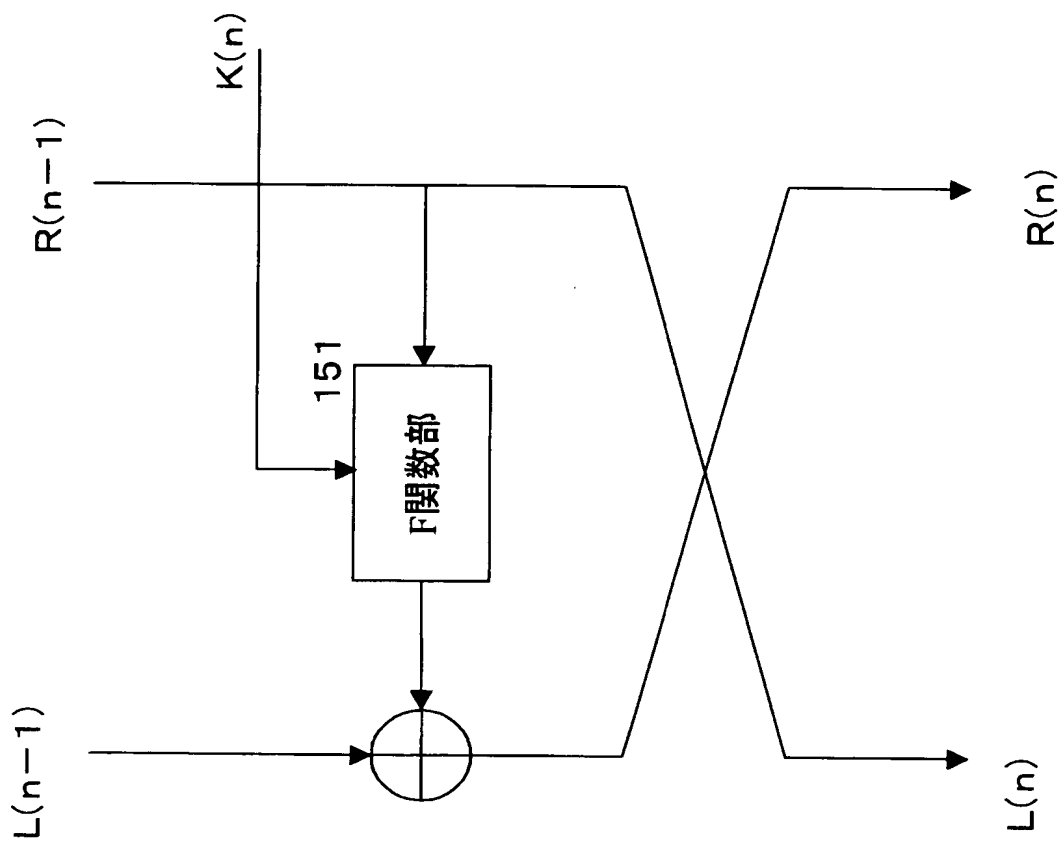
- 511 入力部
- 512 出力部
- 513 通信部
- 514 リムーバブル記憶媒体
- 521 バス
- 522 入出力インタフェース

【書類名】 図面

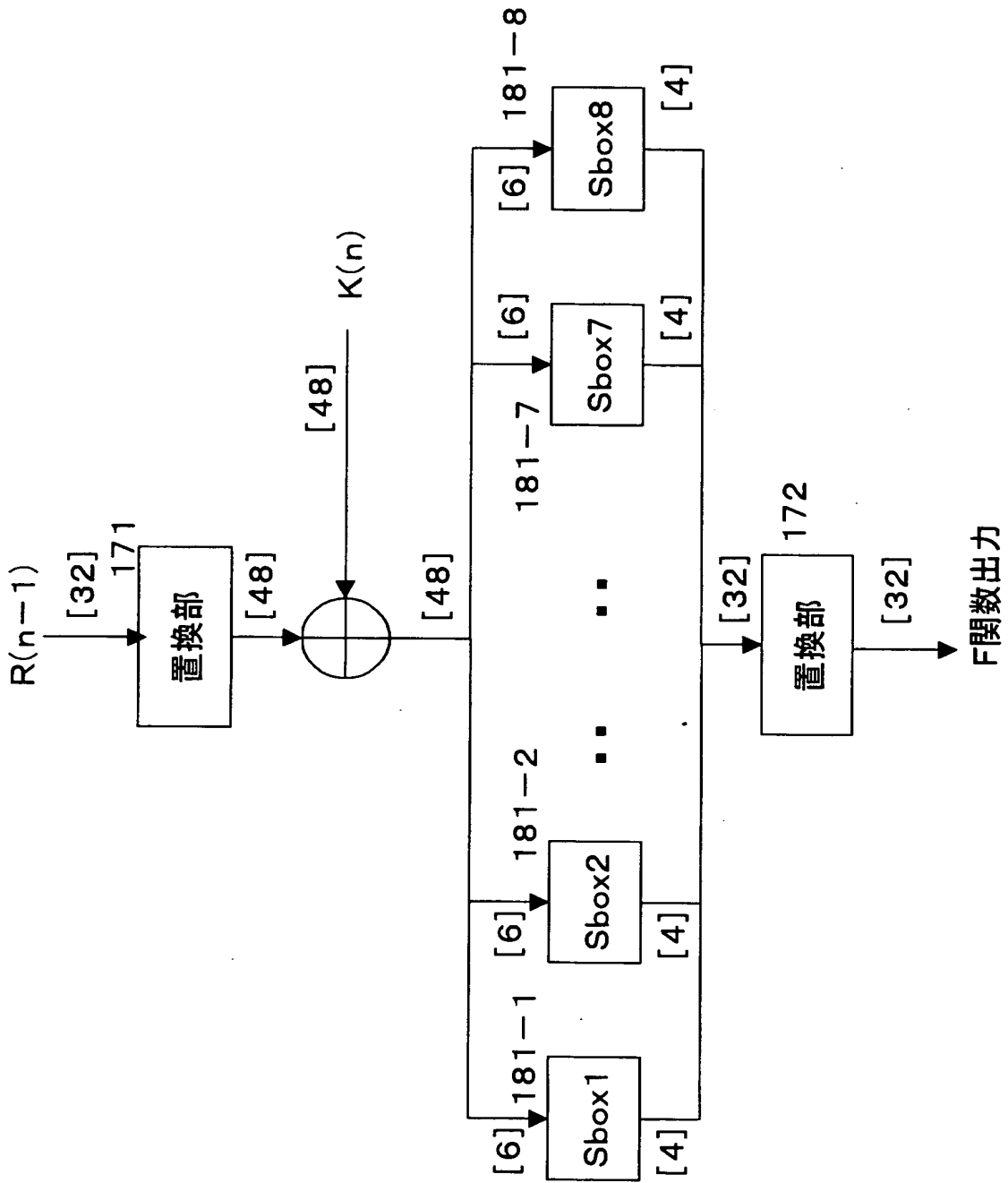
【図1】



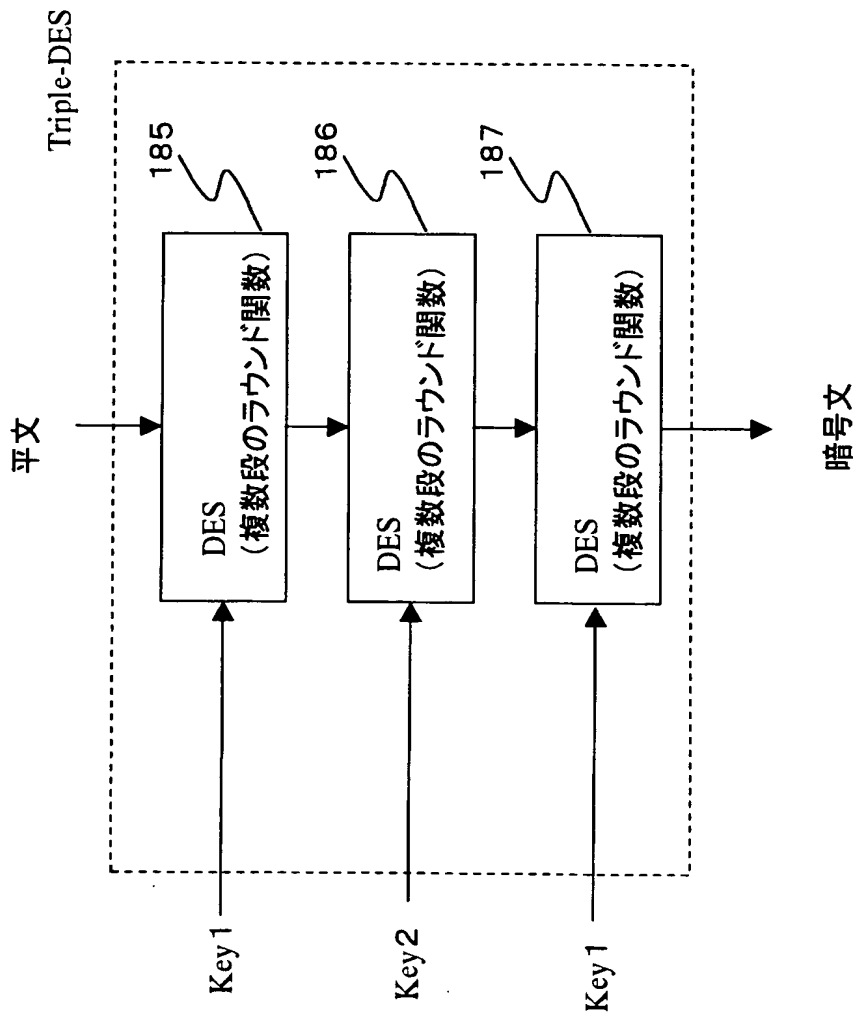
【図 2】



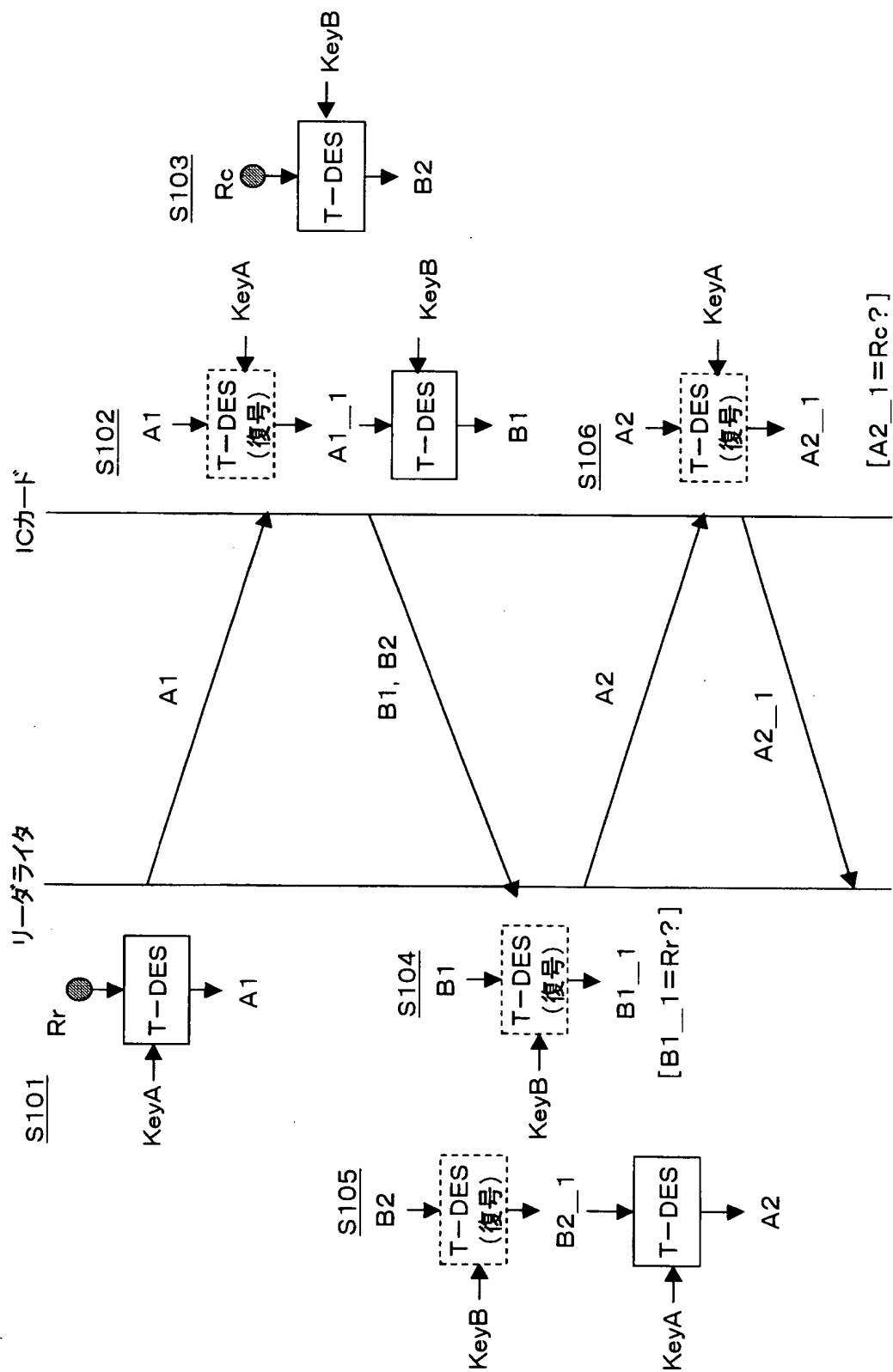
【図3】



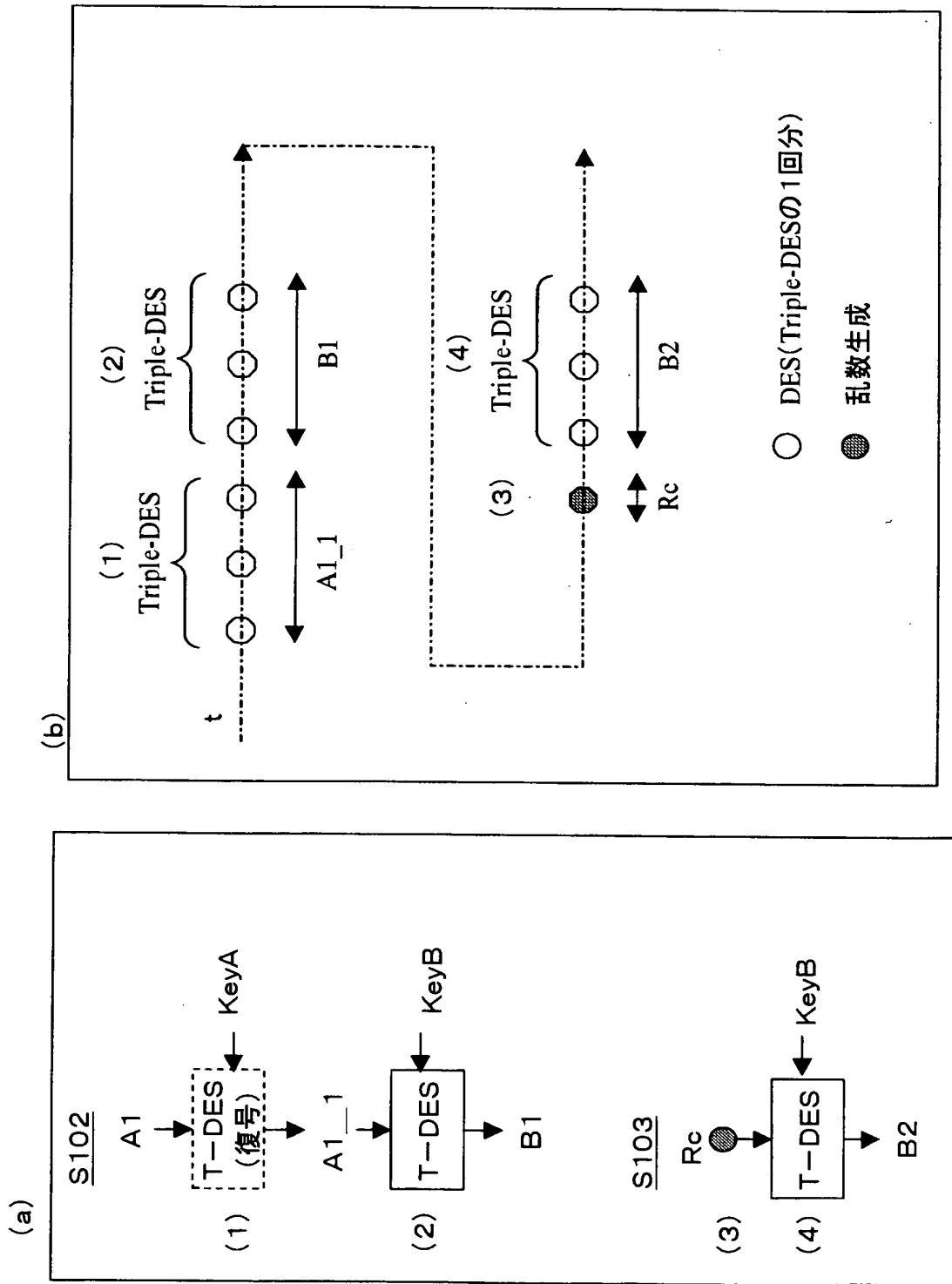
【図 4】



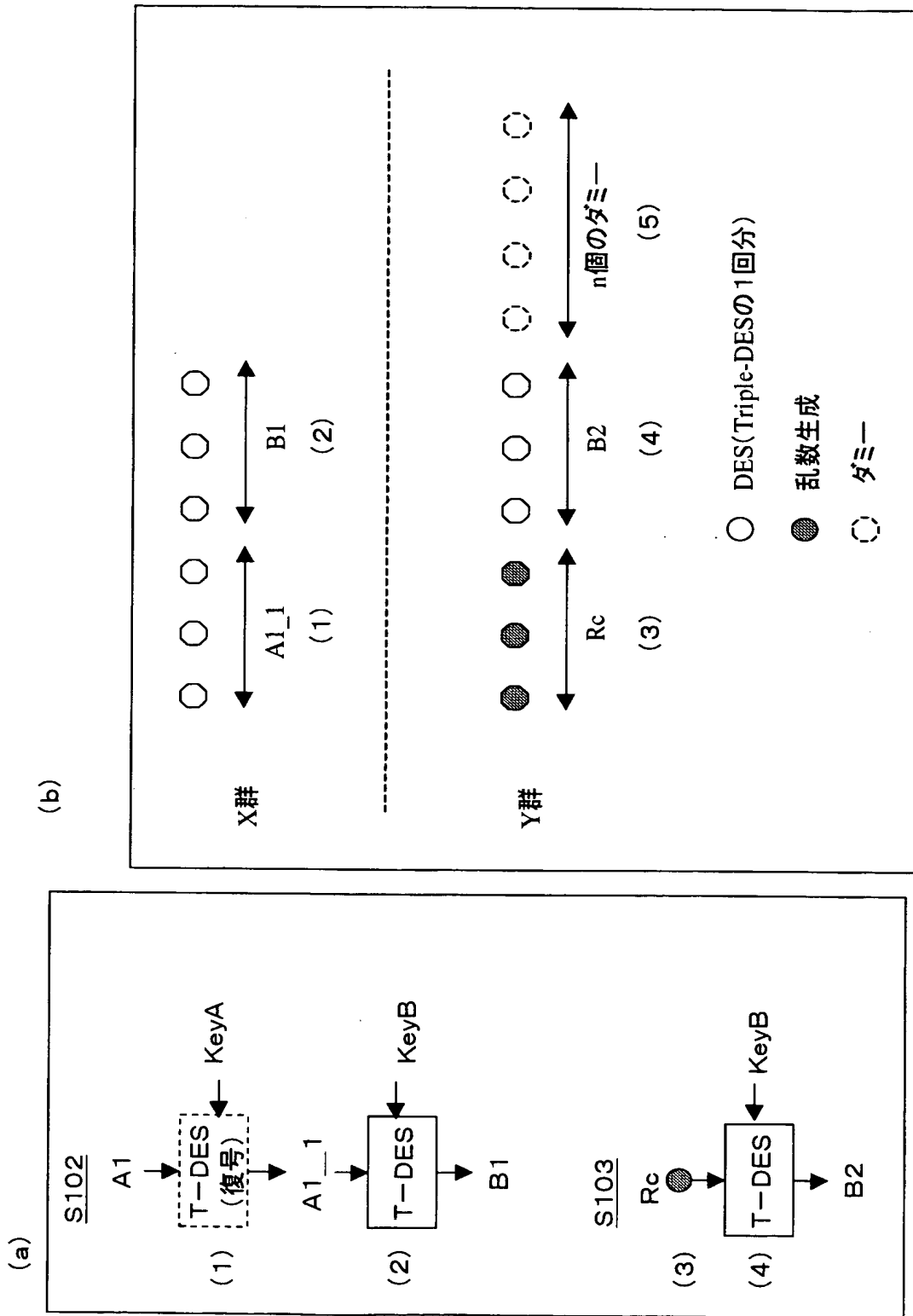
【図5】



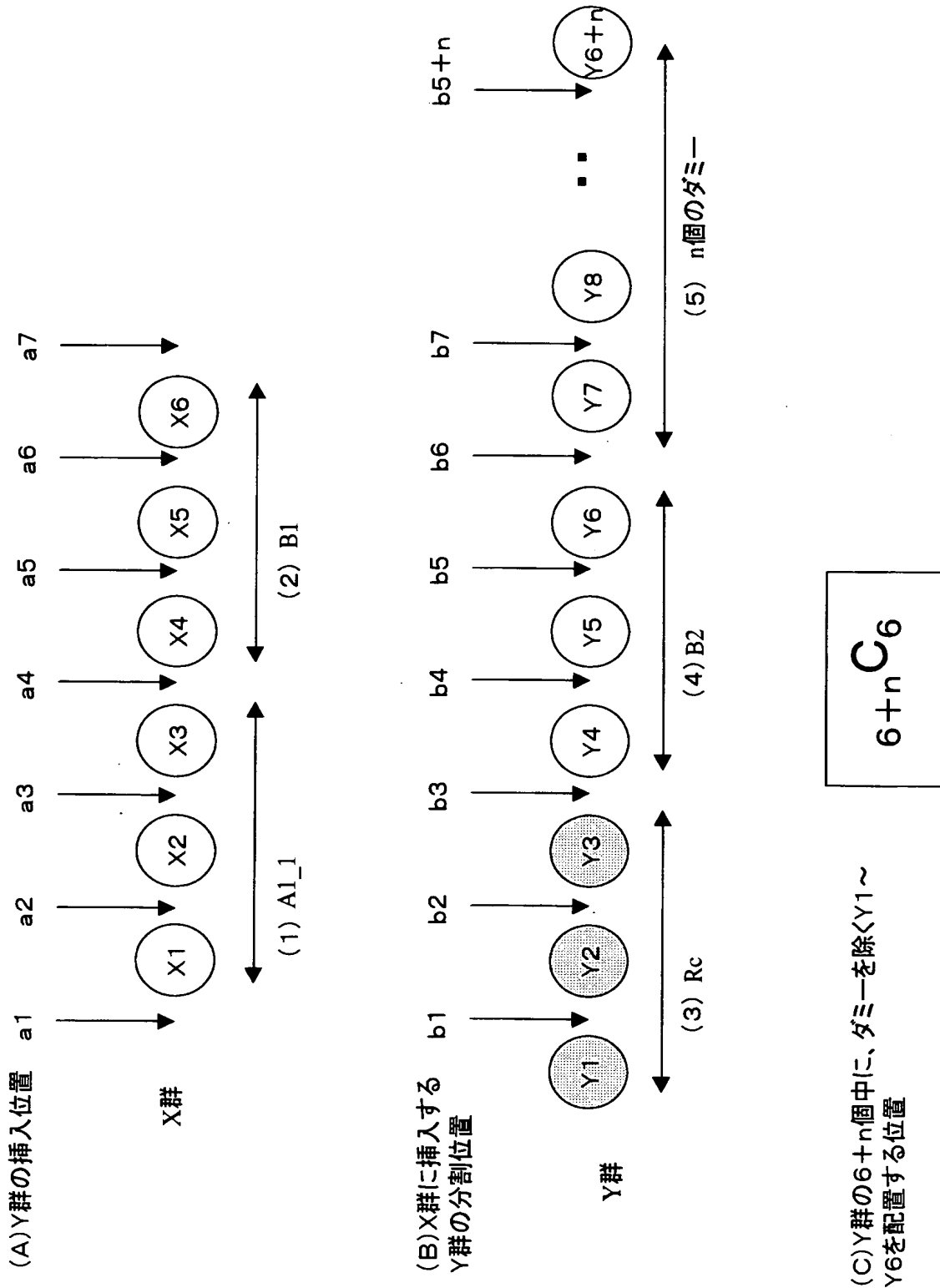
【図6】



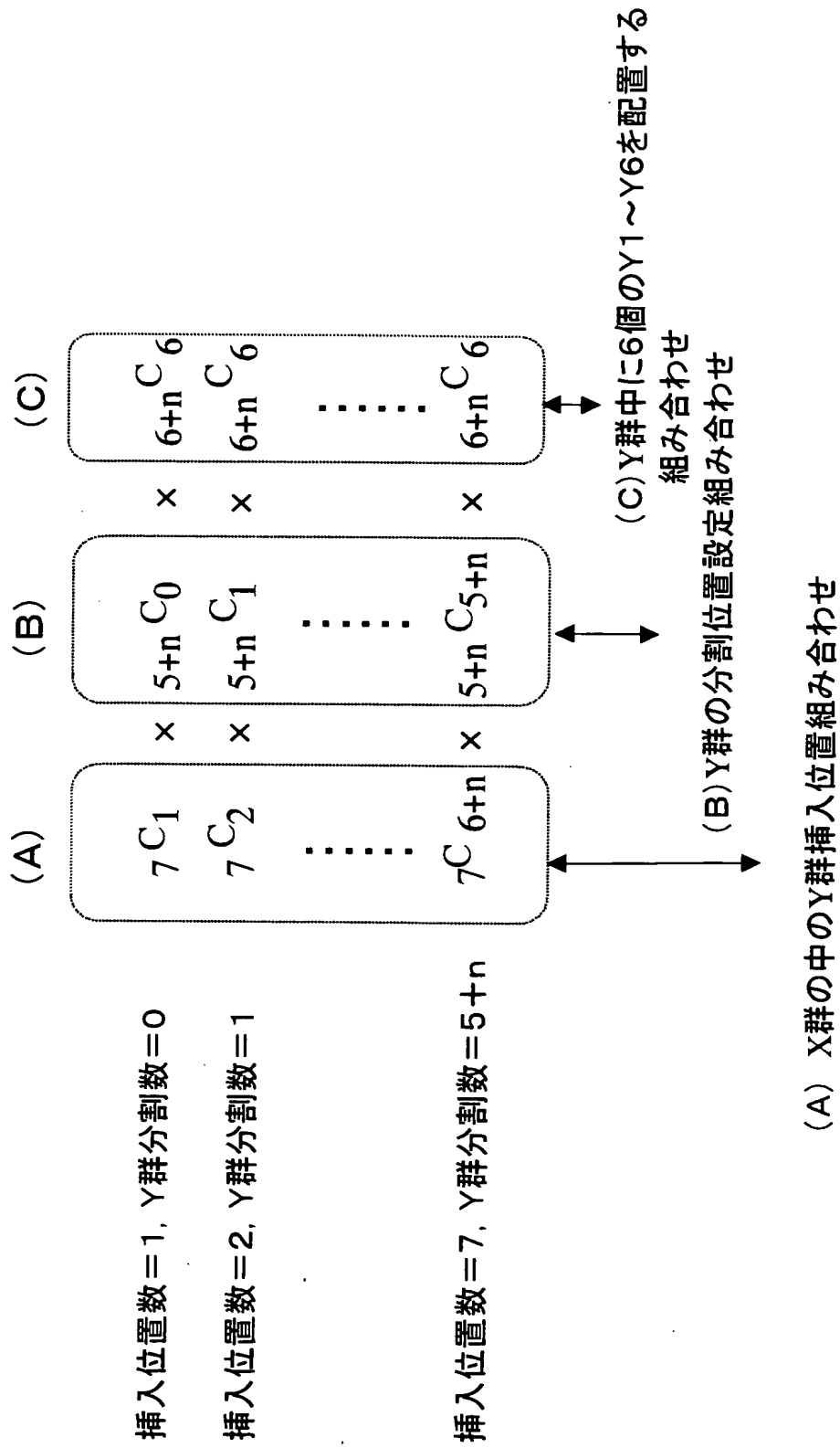
【図 7】



【図8】



【図9】



挿入位置数=1, Y群分割数=0

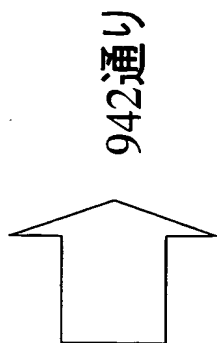
挿入位置数=2, Y群分割数=1

挿入位置数=7, Y群分割数=5+n

【図10】

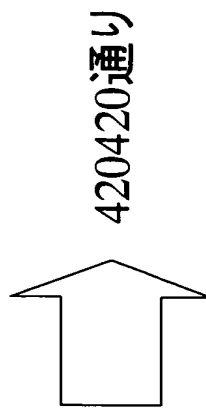
(a) ダミ一数: n=0

$$\begin{aligned}
 {}_7C_1 \times {}_5C_0 \times 1 &= 7 \times 1 \times 1 = 7 \\
 {}_7C_2 \times {}_5C_1 \times 1 &= 21 \times 5 \times 1 = 105 \\
 {}_7C_3 \times {}_5C_2 \times 1 &= 35 \times 10 \times 1 = 350 \\
 {}_7C_4 \times {}_5C_3 \times 1 &= 35 \times 10 \times 1 = 350 \\
 {}_7C_5 \times {}_5C_4 \times 1 &= 21 \times 5 \times 1 = 105 \\
 {}_7C_6 \times {}_5C_5 \times 1 &= 7 \times 1 \times 1 = 7
 \end{aligned}$$

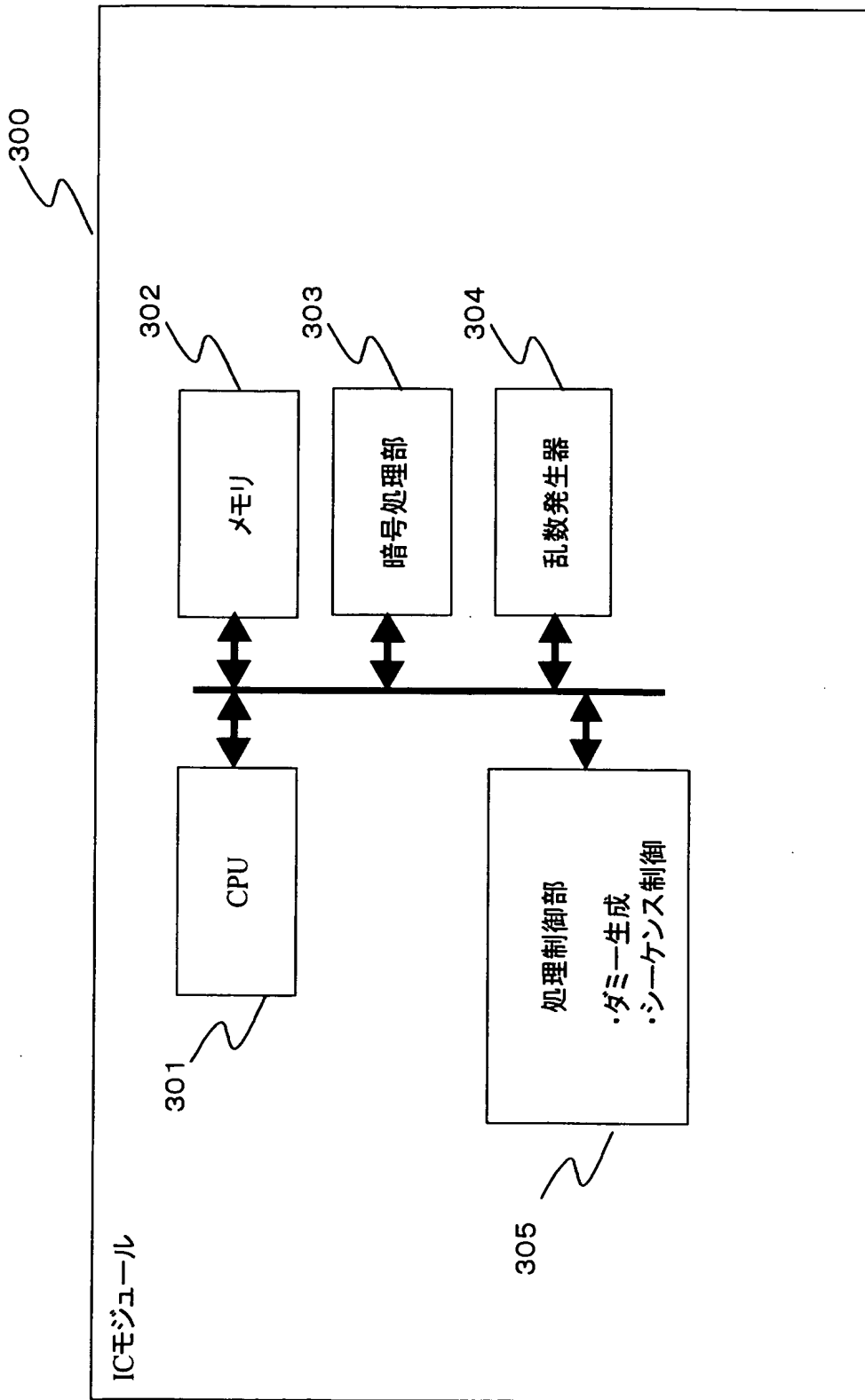


(b) ダミ一数: n=3

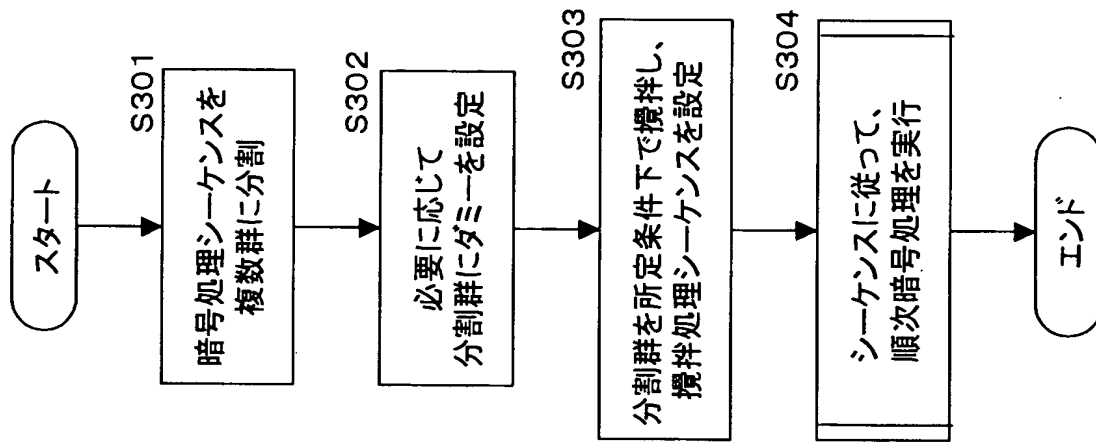
$$\begin{aligned}
 {}_7C_1 \times {}_8C_0 \times {}_9C_6 &= 7 \times 1 \times 84 = 588 \\
 {}_7C_2 \times {}_8C_1 \times {}_9C_6 &= 21 \times 8 \times 84 = 14112 \\
 {}_7C_3 \times {}_8C_2 \times {}_9C_6 &= 35 \times 28 \times 84 = 82320 \\
 {}_7C_4 \times {}_8C_3 \times {}_9C_6 &= 35 \times 56 \times 84 = 164640 \\
 {}_7C_5 \times {}_8C_4 \times {}_9C_6 &= 21 \times 70 \times 84 = 123480 \\
 {}_7C_6 \times {}_8C_5 \times {}_9C_6 &= 7 \times 56 \times 84 = 32928 \\
 {}_7C_7 \times {}_8C_6 \times {}_9C_6 &= 1 \times 28 \times 84 = 2352
 \end{aligned}$$



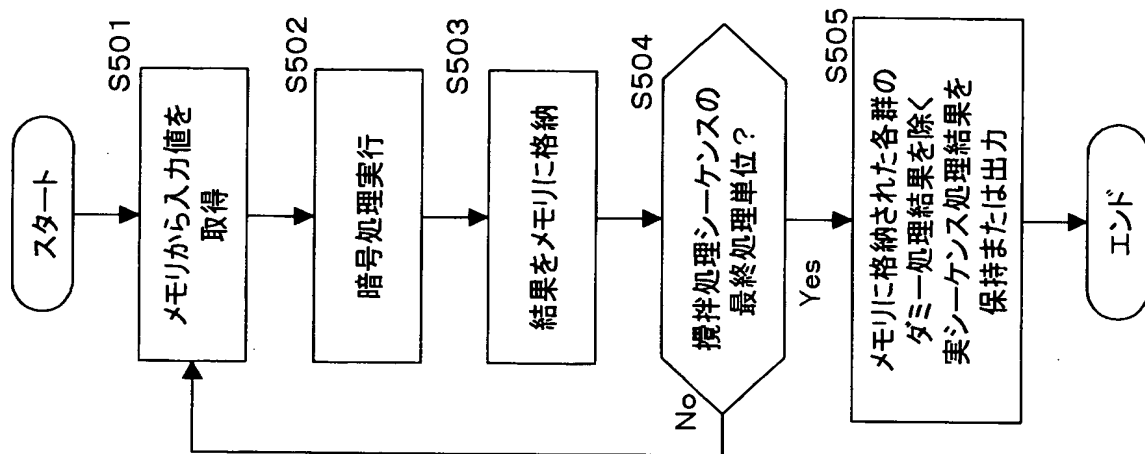
【図11】



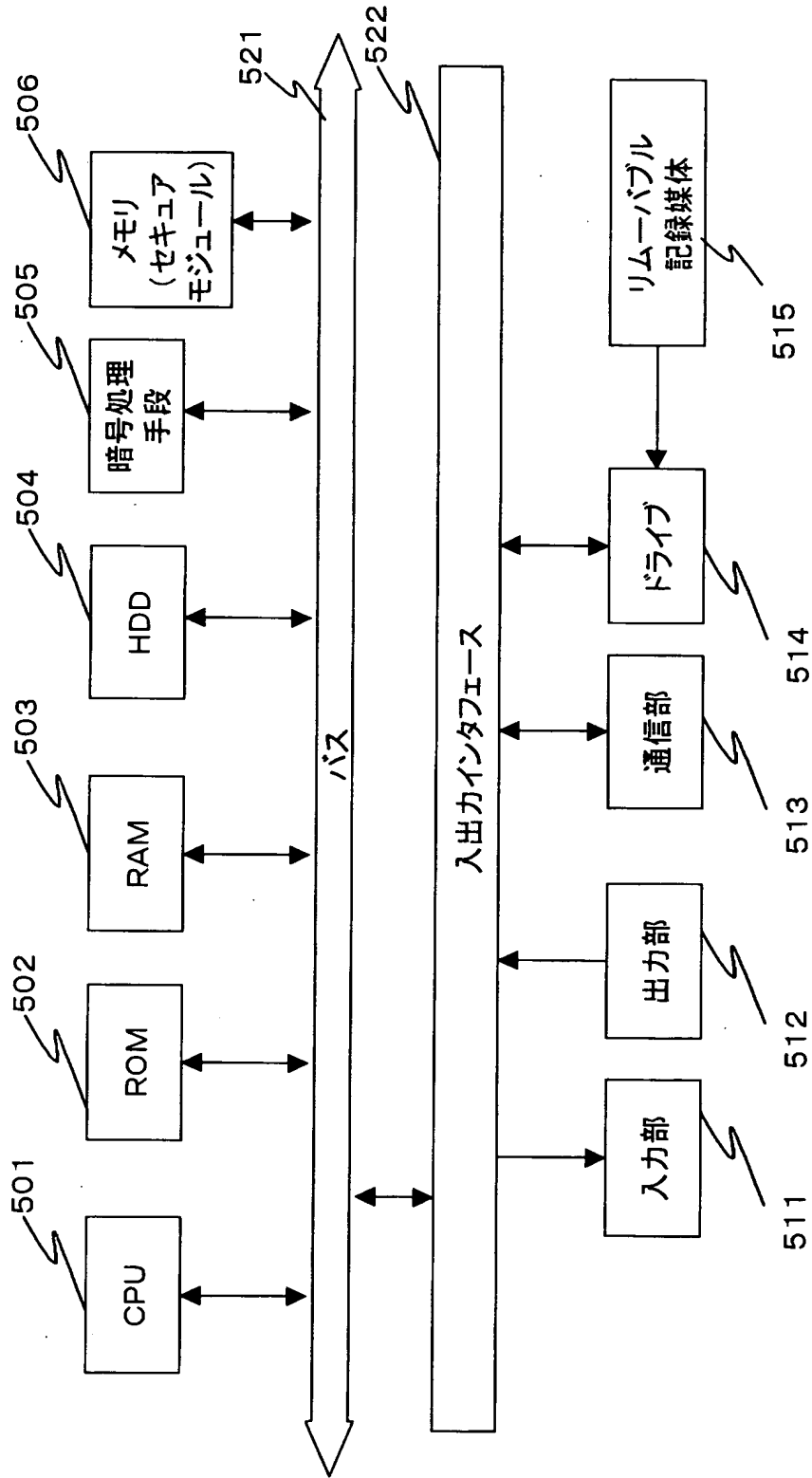
【図 12】



【図13】



【図 14】



【書類名】 要約書

【要約】

【課題】 電力解析による暗号解析の困難性を著しく高めることを可能とした暗号処理装置および方法を提供する。

【解決手段】 オリジナルの暗号処理シーケンスを複数の群へ分割するとともに、必要に応じてダミー設定を実行して処理順を攪拌することで、数百～数万種類の異なる攪拌暗号処理シーケンスの設定を可能とし、これら多数の設定可能なシーケンスから選択したシーケンスを実行する。本構成により、選択された攪拌暗号処理シーケンスの実行毎に、オリジナルの暗号処理シーケンスの持つ規則的な処理に伴う消費電力変動とは全く異なる消費電力変動を発生させることが可能となり、電力解析による暗号解析の困難性を著しく高めることができる。

【選択図】 図 8

特願 2003-001647

出願人履歴情報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住所

東京都品川区北品川6丁目7番35号

氏名

ソニー株式会社